УДК 004.9

СИДОРЕНКО А. В., ЖУКОВЕЦ Д. А., БГУ

ЭЛЕМЕНТЫ ДИФФЕРЕНЦИАЛЬНОГО И ЛИНЕЙНОГО КРИПТОАНАЛИЗА АЛГОРИТМА ШИФРОВАНИЯ С ИСПОЛЬЗОВАНИЕМ ДИНАМИЧЕСКОГО ХАОСА

Белорусский государственный университет

В данной работе проведена оценка устойчивости разработанного алгоритма шифрования на основе динамического хаоса, а так же рассмотрены основные принципы реализации линейного и дифференциального криптоанализа

In this paper we assessed the sustainability of the encryption algorithm based on dynamic chaos, as well as the basic principles for the implementation of linear and differential cryptanalysis

Современная криптография должна обеспечивать защиту, в том числе, критически важной, информации не только от структур других государств, но и транснациональных корпораций. В настоящее время в созданном нами информационном обществе она становится практически центральным инструментом для обеспечения достоверности, конфиденциальности и целостности передаваемой информации.

Объем циркулирующей в обществе информации стабильно возрастает. Популярность всемирной сети Интернет в последние годы способствует ежегодному удвоению информации. Фактически, на начало 21 века человечеством создана информационная цивилизация, в которой от успешной работы средств обработки информации зависит его благополучие и даже, в некотором смысле, его выживание.

Произошедшие за этот период изменения можно охарактеризовать следующим образом:

• объемы обрабатываемой информации возросли за полвека практически на несколько порядков;

• доступ к определенным данным позволяет контролировать значительные материальные и финансовые ценности; информация приобрела стоимость, которую можно рассчитать;

• характер обрабатываемых данных стал чрезвычайно многообразным и значительно отличается от текстового представления;

• характер информационных взаимодействий усложнился, возникли новые задачи в сфере защиты информации;

• субъектами информационных процессов являются люди, а также созданные ими автоматизированные системы, действующие по заложенной в них программе;

• вычислительные мощности современных компьютеров подняли на совершенно новый уровень как возможности по реализации шифров, ранее немыслимых из-за своей высокой сложности, так и возможности аналитиков по их взлому.

В современном мире информационный ресурс стал одним из наиболее мощных рычагов экономического развития. Владение информацией необходимого качества в нужное время и в нужном месте является залогом успеха в любом виде деятельности. Монопольное обладание определенной информацией оказывается зачастую решающим преимуществом в конкурентной борьбе и предопределяет, тем самым, высокую цену «информационного фактора».

Для защищаемой информации характерны следующие признаки:

• имеется какой-то определенный круг законных пользователей, которые имеют право владеть этой информацией;

• имеются незаконные пользователи, которые стремятся овладеть этой информацией с тем, чтобы обратить ее себе во благо, а законным пользователям во вред.

Решение задач защиты информации становится определяющим в современном обществе

В данной работе проведены исследования разработанного нами алгоритма шифрования, описание которого приведено в работе [1]

Устойчивость к линейным атакам (лавинный эффект)

В качестве исследуемого изображения выбран полученный со спутника снимок факультета радиофизики и компьютерных технологий БГУ размером 512×512 пикселей (рис. 1)

Для проверки чувствительности к открытому тексту, мы зашифруем цветное изображение. Затем, изменяем один бит в исходном изображении. Модифицированное изображение зашифруем снова с помощью того же ключа. Показатель изменения бит для пары зашифрованных изображений получают следующим образом [2] [3]:

$$\text{Кол-во бит изменивших значение} = \frac{\text{Показатель изменения бит}}{\text{Общее количество бит}}$$

Из результатов тестирования разработанного алгоритма, при изменении одного бита в исходном изображении меняется 49.997843% бит в зашифрованном изображении, что очень близко к идеальному значению в 50%. Таким образом, алгоритм является устойчивым к линейным атакам.

Устойчивость к дифференциальным атакам

Основываясь на принципах криптологии, хороший алгоритм шифрования должен быть чувствительным к открытому тексту. Чувствительность алгоритма шифрования может быть

Рис. 1. Снимок факультета радиофизики и компьютерных технологий БГУ, с прилегающей к нему территорией

количественно оценена следующими параметрами: процент пикселей изменивших значение (Number of Pixels Change Rate (NPCR)) и среднее изменение интенсивности (Unified Average Changing Intensity (UACI)). Соответственно, NPCR и UACI определяются по следующим формулам:

$$NPCR = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)\cdot 100\%$$

$$UACI = \frac{1}{255MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|C_1(i,j) - C_2(i,j)\right|\cdot 100\%$$

где, $D(i,j) = \begin{cases} 0, \text{если } C_1(i,j) = C_2(i,j) \\ 1, \text{если } C_1(i,j) \neq C_2(i,j) \end{cases}$ $C_1(i,\ j)$ и $C_2(i,j)$ значения пикселей двух зашифрованных изображений в положении $(i,\ j)$ M и N представляют собой номера строки и столбца изображения.

Таблица 1. **Результаты расчета параметров NPCR и UACI для двух зашифрованных цветных изображений факультета при условии, что исходные изображения отличались одним пикселем (R – красный цвет, G – зеленый цвет, B – синий цвет)**

Изменение в пикселе	NPCR				UACI			
	R	G	B	Идеал	R	G	B	Идеал
(1,1)	99,6	99,61	99,62	99,61	33,39	33,46	33,41	33,46
(512,1)	99,59	99,6	99,61		33,46	33,43	33,46	
(1,512)	99,63	99,63	99,6		33,47	33,39	33,46	
(512,512)	99,61	99,62	99,62		33,52	33,45	33,5	
(256,256)	99,59	99,6	99,61		33,52	33,47	33,52	

В дополнение, идеальные значения *NPCR* и *UACI* могут быть рассчитаны по следующим формулам [4]:

$$NPCR_{ideal} = (1 - 2^{-n}) \cdot 100\%$$

$$UACI_{ideal} = \frac{1}{2^{2n}} \frac{\sum_{i=1}^{2^n - 1} i(i+1)}{2^n - 1} \cdot 100\% =$$

$$= \frac{1}{3}(1 + 2^{-n}) \cdot 100\%$$

где n – количество битов используемых для представления одного пикселя. В сером изображении используется 8 бит на пиксель, $n = 8$.

Из результатов, приведенных в табл. 1, можно заметить, что получаемые значения NPCR и *UACI* колеблются около идеальных значений. Из этого следует, что алгоритм является чувствительным к малым изменениям в исходном изображении и устойчивым к дифференциальным атакам.

Элементы дифференциального криптоанализа

Основной объект, который исследуется в дифференциальном криптоанализе – это пары блоков текста A и B с определенной разностью $A \oplus B$ [5]. Если информация о том, как связаны входная разность (между блоками открытого текста) и выходная разность (между блоками шифртеста), отсутствует, то все выходные разности равновероятны. Однако если удается установить, что некоторая входная разность Δ_{in} приводит к некоторой выходной разности Δ_{out} с вероятностью p большей, чем остальные, то это может быть использовано для отыскания подключей шифра. Пара (Δ_{in}, Δ_{out}) называется *дифференциалом*, а совокупность дифференциалов на различных раундах называется *характеристикой*. Если Δ_{out} содержит неизвестные биты, то дифференциал называется *усеченным*.

Для совершенного шифра со 128-битовым блоком при любой входной разности выходная разность примет некоторое фиксированное значение с вероятностью 2^{-128}. Таким образом, если в процессе анализа шифра обнаружится, что определенная входная разность приводит к определенной выходной разности с вероятностью больше чем 2^{-128} (например, 2^{-100}), то эта информация может быть использована с целью отыскания его подключей. Количество текстов, требуемых для реализации атаки, пропорционально $1/p$. В результате проведенной работы нами было получено распределение вероятностей для всех входных разностей функции шифрования F (см. табл. 2).

Таблица 2. **Распределения вероятностей дифференциальных характеристик для входных разностей F-блока**

№ п/п	Вероятность, p	Кол-во разностей
1	1	1
2	0,011–0,012	1
3	0,005–0,011	0
4	0,004–0,005	99
5	0,003–0,004	155
6	0,002–0,003	28
7	0,001–0,002	228
8	0,0004–0,001	0
9	0,0003–0,0004	1
10	0,0002–0,0003	5013
11	0,0001–0,0002	7837964
12	0–0,0001	4287123806

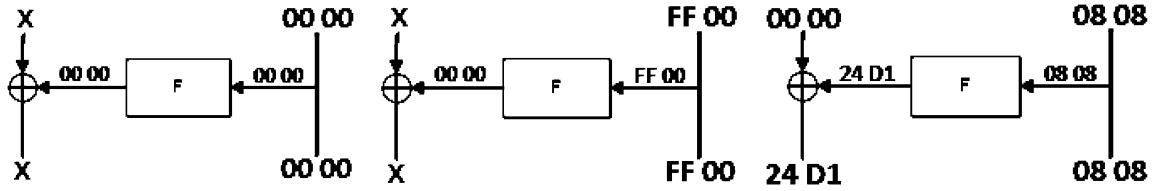
Видно, что лишь малой части входных разностей на выходе будут соответствовать одинаковой разности.

Чтобы показать вероятность, с которой одна входная разность создает определенную разность на выходе, вводят такое понятие, как *характеристика раунда*.

Следует обратить внимание на то, что характеристика одна и та же для каждого раунда, так как любое отношение, которое включает разности, не зависит от ключей раунда. На рис. 2 представлены только три из существующих характеристик. В каждой характеристике мы разделили входные разности и разности выхода в левые и правые секции. Каждая разность состоит из 4 шестнадцатеричных цифр (2 байт).

Все характеристики определяются с помощью разработанной нами компьютерной программы. На рис. 2, *а* показано, что входная разность (xxxx, 0000) дает на выходе разность (xxxx, 0000) с вероятностью 1 (здесь xxxx – любая разность). Из рис. 2, *б* видно, что входная разность (xxxx, FF00) дает разность на выходе (xxxx, FF00) с вероятностью 0,0116882. Наконец, рисунок 2, *в* показывает, что входная разность (0000,0808) дает разность на выходе (24D1,0808) с вероятностью 2^{-12}.

После создания и хранения одноразундовых характеристик криптоаналитик может комби-



а *б* *в*

Рис. 2. Характеристики раунда для дифференциального криптоанализа при различных входных разностях: *а* – вероятность характеристики $p = 1$; *б* – вероятность характеристики $p = 0.0116882$; *в* – вероятность характеристики $p = 2^{-12}$

нировать разное количество раундов, чтобы создать множественную характеристику раунда. На рис. 3 приведена характеристика трехраундового алгоритма. Характеристики, показанные в первом и третьем раундах, аналогичны рис. 2, *б*. Характеристика во втором раунде – аналогична рис. 2, *а*.

Вероятность такой характеристики равна произведению вероятностей одноразундовых характеристик $p = 0{,}0116882 \cdot 1 \cdot 0{,}0116882 = 0{,}0001366$.

Однако данный метод не учитывает малую часть возможных ситуаций, когда на вход поступает разность (0000, FF00), на выходе получается разность (0000, FF00), но на втором раунде используется характеристика с вероятностью $p \neq 1$. Для точного расчета вероятности многораундовой характеристики нами было реализовано программное обеспечение.

Результаты расчетов с использованием разработанной компьютерной программы приведены в табл. 3.

Таблица 3. **Результаты расчета вероятности многораундовой характеристики, для различного количества раундов**

Кол-во раундов	Входная разность	Выходная разность	Вероятность, p
1	00 00 FF 00	00 00 FF 00	1,16882E–02
2	00 00 FF 00	FF 00 00 00	1,16882E–02
3	00 00 FF 00	00 00 FF 00	1,36787E–04
4	00 00 FF 00	FF 00 00 00	1,36787E–04
5	00 00 FF 00	00 00 FF 00	1,64052E–06
6	00 00 FF 00	FF 00 00 00	1,64052E–06
7	00 00 FF 00	00 00 FF 00	2,28174E–08
8	00 00 FF 00	FF 00 00 00	2,28174E–08
9	00 00 FF 00	00 00 FF 00	9,31323E–10
10	00 00 FF 00	FF 00 00 00	9,31323E–10
11	00 00 FF 00	00 00 FF 00	4,65661E–10
12	00 00 FF 00	FF 00 00 00	4,65661E–10
13	00 00 FF 00	00 00 FF 00	9,31323E–10
14	00 00 FF 00	FF 00 00 00	9,31323E–10
15	00 00 FF 00	00 00 FF 00	4,65661E–10

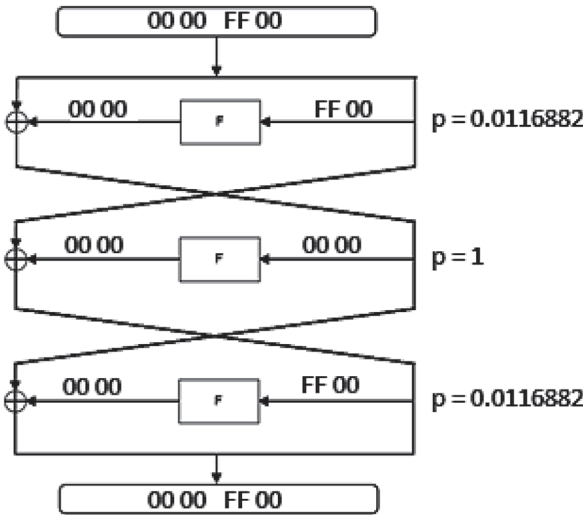


Рис. 3. Трехраундная характеристика для дифференциального криптоанализа

Для нахождения ключа шифрования при использовании одного раунда применяем следующий алгоритм (обозначения представлены на рис. 4):

1) Строим уравнения функции шифрования

$$(f_1(X_1 \oplus K_1;\ X_2 \boxplus K_3) \boxplus K_2) \oplus (f_1(X_1^* \oplus K_1;\ X_2^* \boxplus K_3) \boxplus K_2) = \Delta Y_1,$$

$$f_2(X_2 \boxplus K_3; f_1(X_1 \oplus K_1;\ X_2 \boxplus K_3) \oplus f_2(X_2^* \boxplus K_3;\ f_1(X_1^* \oplus K_1;\ X_2^* \boxplus K_3)) = \Delta Y_2,$$

где $X_1^* = X_1 \oplus \Delta X_1$; $X_2^* = X_2 \oplus \Delta X_2$; Δ – разность.

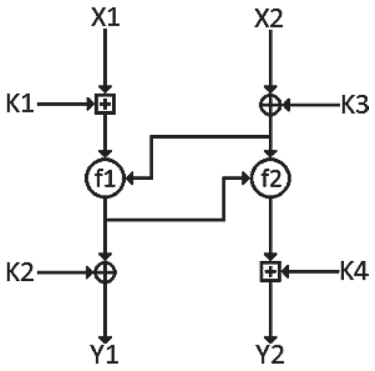


Рис. 4. Внутренняя структура раундовой функции F

2) Перебирая различные пары входных текстов с заданной разностью и различные ключи (K_1, K_2, K_3, K_4), будем подбирать несколько вариантов для ключа. Для всех вариантов ключа можно завести счетчики, и если какая-либо пара предлагает данный вариант в качестве верного ключа, будем увеличивать соответствующий счетчик. Ключ, которому соответствует самый большой счетчик, с высокой вероятностью является верным.

Чтобы выделить правильный ключ, необходима характеристика с соответствующей вероятностью и достаточное количество пар, чтобы гарантировать наличие правильных пар. Число необходимых пар определяется вероятностью характеристики, числом бит ключа, которые мы хотим определить и уровнем идентификации ошибочных пар (они не вносят вклада в счетчики, так как отбрасываются ранее). Пусть мы ищем k бит ключа, тогда у нас имеется 2^k счетчиков. Среднее значение счетчика равно $m\alpha\beta/2^k$, где m – число используемых пар, α – средняя добавка к счетчикам для одной пары, β – отношение пар которые вносят вклад в счетчики ко всем парам (в том числе отброшенным). Тогда отношение сигнал/шум определяется

$$S / N = \frac{mp}{m\alpha\beta / 2^k} = \frac{2^k p}{\alpha\beta}$$

где p – вероятность характеристики, mp – число правильных пар.

Заметим, что отношение сигнал/шум для расчетной схемы не зависит от общего числа пар. Число необходимых правильных пар – в общем, является функцией отношения сигнал/шум. Экспериментально было получено, что если $S / N = 1 – 2$, необходимо 20–40 вхождений правильных пар. Если же отношение намного выше, то даже 3–4 правильные пары может быть достаточно. Наконец, когда оно значительно ниже, необходимо огромное число пар.

В результате проведенных расчетов с использованием разработанной нами компьютерной программы для одного раунда F функции с входным значением $X = \{00,04\}$ и выходным $Y = \{01,05\}$ были получены следующие значения:

$\beta = 2^0$; $\alpha = 3\times2^8$; $k = 24$; $p = 2^{-15}$; $S/N = 2/3$;

Следовательно, необходимо вхождение порядка 60 правильных пар для проведения криптоанализа данного раунда. Всего понадобится $60/2^{-15} \approx 2^{21}$ текстов для криптоанализа раунда.

Для раунда F функции с входным значением $X = \{FF,00\}$ и выходным $Y = \{00,00\}$ были получены следующие значения:

$\beta = 2^0$; $\alpha = 3\times2^{16}$; $k = 24$; $p = 0{,}01169$; $S/N = 1$;

Следовательно, для проведения криптоанализа необходимо порядка 40 вхождений правильных пар. Всего понадобится $40/0{,}01169 \approx 3425$ текстов для криптоанализа раунда.

В качестве примеров были выбраны варианты с минимальной и максимальной вероятностью. Как видно из приведенных результатов количество текстов необходимых для криптоанализа одного раунда алгоритма в обоих случаях довольно высоко

Элементы линейного криптоанализа

Линейный криптоанализ заключается в поиске линейной аппроксимации между открытым текстом, соответствующим зашифрованным текстом и ключом шифрования. Оказывается, можно представить функцию шифрования в виде системы уравнений, которые выполняются с некоторой вероятностью p. Так как уравнения, полученные в ходе анализа криптоалгоритма, являются вероятностными, то их называют линейными статистическими аналогами. Эффективность линейного статистического аналога определяется отклонением, которое вычисляется как $\Delta = |1 – 2p|$. При этом для успешного анализа вероятность уравнений p должна быть, как можно дальше удалена от значения 1/2 (то есть приближаться либо к нулю, либо к единице). Полученные значения в дальнейшем используются для нахождения искомых значений ключа шифрования.

Линейная аппроксимация функции шифрования в общем виде выглядит следующим образом [6]:

$$P_{i1} \oplus ... \oplus P_{il} \oplus C_{j1} \oplus ... \oplus C_{jm} = K_{k1} \oplus ... \oplus K_{kn}$$

где P_n, C_n, K_n – n-ые биты открытого текста, зашифрованного текста и ключа.

Вероятность p справедливости такого соотношения для произвольно выбранных бит открытого текста, зашифрованного текста и ключа примерно равна 1/2.

Пусть на вход функции F i-го раунда шифрования поступает значение X, на выходе

функции F i-го раунда шифрования образуется значение Y. Используемый бит для значений X и Y будем заключать в квадратные скобки.

Для построения линейной аппроксимации одного раунда шифрования были использованы вычислительные мощности суперкомпьютера СКИФ-БГУ. Так же, для уменьшения времени расчёта линейных аппроксимаций была упрощена структурная схема раундовой функции F (см. рис. 5)

Результаты, полученные с использованием разработанной нами компьютерной программы, позволили определить следующие аппроксимации:

$$X1[0,3,4,5,6,7] \oplus K1[0,3,4,5,6,7] \oplus X2[1,3,5] \oplus$$
$$\oplus K3[1,3,5] \oplus Y1[0,1] \oplus Y1[2,3,4,5] \oplus$$
$$\oplus K2[0,1,2,3,4,5] \oplus Y2[1,2,3,4,5,6] \oplus$$
$$\oplus K4[1,2,3,4,5,6] = 1$$

$$X1[1,2,3,4,6] \oplus K1[1,2,3,4,6] \oplus X2[4,5] \oplus$$
$$\oplus K3[4,5] \oplus Y1[1] \oplus Y1[4,5,7] \oplus K2[1,4,5,7] \oplus$$
$$\oplus Y2[0,1,2,5,6] \oplus K4[0,1,2,5,6] = 1$$

Вероятность выполнения полученных линейных аппроксимаций, а так же получаемые при этом отклонения соответственно равны:

$$p = 0{,}489380,\ \Delta = 0{,}02124$$
$$\text{и } p = 0{,}510376,\ \Delta = 0{,}020752.$$

Количество текстов необходимых для криптоанализа одного раунда

$$\left|0{,}5104 - \frac{1}{2}\right|^{-2} = 1{,}13 \cdot 2^{13}.$$

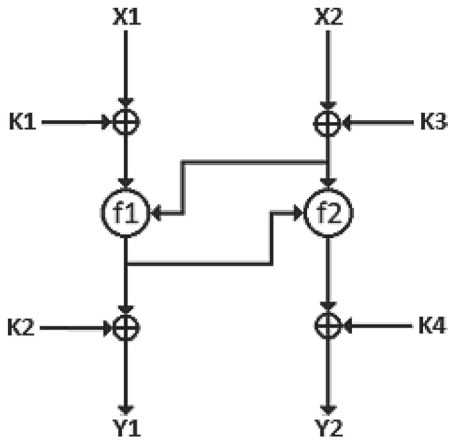


Рис. 5. Внутренняя структура упрощенной раундовой функции F

Заключение

В результате выполнения работы нами проведен анализ устойчивости алгоритма шифрования данных на основе динамического хаоса. При этом проведены исследования по реализации элементов дифференциального и линейного крипто-анализа при одном раунде шифрования. Разработано и использовано программное обеспечение для проведения как для дифференциального, так и линейного криптоанализа.

Результаты анализа данных, полученных в результате тестирования, показали, что алгоритм шифрования является устойчивым к вскрытию разработанного шифра, что было подтверждено использованием элементов дифференциального и линейного криптоанализа.

Литература

1. **Сидоренко А. В.** Блочный алгоритм шифрования на основе динамического хаоса / Сидоренко А. В., Жуковец Д. А. // *Весник БГУ.* – 2015.

2. **Seyedzadeh S. M.** Image Encryption Algorithm Based on Choquet Fuzzy Integral with Self-Adaptive Pseudo-Random Number Generator / Seyedzadeh S. M., Hashemi Y. // *11th International Conference on Intelligent Systems Design and Applications (ISDA), Cordoba, 22–24 Nov. 2011* – Cordoba, 2011. – P. 642–647.

3. **Seyedzadeh S. M.** RGB Color Image Encryption based on Choquet Fuzzy Integral / Seyedzadeh S. M., Norouzi B., Mirzakuchaki S. // *The Journal of Systems and Software.* – 2014 – Vol. 97 – P. 128–139.

4. A novel image encryption scheme based on an improper fractional-order chaotic system / Jianfeng Zhao [et al.] // *Nonlinear Dynamics* – 2015.

5. **Biham E.** Differential Cryptanalysis of DES-like Cryptosystems / Biham E., Shamir A. // *Lecture Notes in Computer Science,* vol. 537, pp. 2–21, 1991.

6. **Matsui M.** Linear Cryptanalysis Method for DES Cipher / Matsui M. // *Lecture Notes in Computer Science,* vol. 765, pp. 386–397, 1994.

Поступила 28.08.15. После доработки 15.09.15

Sidorenko A., Zhukovets L. A.

DIFFERENTIAL AND LINEAR CRYPTOANALYSIS METHODS ELEMENTS FOR ENCRYPTION ALGORITHM BASED ON DYNAMIC CHAOS

In this paper we assessed the sustainability of the encryption algorithm based on dynamic chaos, as well as the basic principles for the implementation of linear and differential cryptanalysis.